Amendments to the CLAIMS:

Without prejudice, this listing of the claims replaces all prior versions and listings of the claims in the present application:

LISTING OF CLAIMS:

1. (Currently Amended) A distributed digital signature generation method for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, said distributed digital signature generation method comprising the steps of:

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputting said partial digital signature or a pair of said digital document and said partial digital signature;

combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

2. (Canceled).

3. (Currently Amended) The distributed digital signature generation method as claimed in claim 1, said method further comprising the step of:

judging whether an incorrect partial digital signature generated by an incorrect partial signature key exists, and identifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

4. (Currently Amended) A distributed digital signature generation method for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, said method comprising the steps of:

each of said partial digital signature generation parts adding one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputting a pair of said digital document with additional information and said partial digital signature;

combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

5. (Canceled).

6. (Original) The distributed digital signature generation method as claimed in claim 4, said method further comprising the step of:

judging whether an incorrect partial digital signature generated by an incorrect partial signature key exist and identifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

7. (Currently Amended) A distributed digital signature generation apparatus for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said distributed digital signature generation apparatus comprising:

a part for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

a part for generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

8. (Canceled).

9. (Original) The distributed digital signature generation apparatus as claimed in claim 7, said apparatus further comprising:

a part for judging whether an incorrect partial digital signature generated by an incorrect partial signature key exists and identifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

10. (Currently Amended) A distributed digital signature generation apparatus for generating a digital signature for a digital document by using a plurality of partial digital

signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said distributed digital signature generation apparatus comprising:

a part for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

a part for generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

11. (Canceled).

12. (Original) The distributed digital signature generation apparatus as claimed in claim 10, said apparatus further comprising:

a part for judging whether an incorrect partial digital signature generated by an incorrect partial signature key exists and specifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

13. (Currently Amended) A digitally signed digital document generation method for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, said digitally signed digital document generation method comprising the steps of:

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputting said partial digital signature or a pair of said digital document and said partial digital signature;

combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined' number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures;

generating an integrated digital signature from a result of said transformation process; and

generating a digital document with digital signature which includes said digital document and said integrated digital signature;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

14. (Currently Amended) A digitally signed digital document generation method for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, said digitally signed digital document generation method comprising the steps of:

each of said partial digital signature generation parts adding one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputting a pair of said digital document with additional information and said partial digital signature;

combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

generating an integrated digital signature from a result of said transformation process; and

generating a digital document with digital signature which includes said digital document and said integrated digital signature;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

15. (Currently Amended) A digitally signed digital document generation apparatus for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said digitally signed digital document generation apparatus comprising:

a part for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial

digital signatures;

a part for generating an integrated digital signature from a result of said transformation process; and

a part for generating a digital document with digital signature which includes said digital document and said integrated digital signature;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

16. (Currently Amended) A digitally signed digital document generation apparatus for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said digitally signed digital document generation apparatus comprising:

a part for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs;

a part for generating an integrated digital signature from a result of said transformation process; and

a part for generating a digital document with digital signature which includes said digital document and said integrated digital signature;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

17. (Currently Amended) A program for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said program comprising:

program code means for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

program code means for generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

18. (Currently Amended) A program for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said program comprising:

program code means for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

program code means for generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

19. (Currently Amended) A computer readable medium storing program code for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said computer readable medium comprising:

program code means for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined

number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

program code means for generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

20. (Currently Amended) A computer readable medium storing program code for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said computer readable medium comprising:

program code means for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

program code means for generating an integrated digital signature from a result of said transformation process;

wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

21. (New) A distributed digital signature generation method for generating a digital signature for a digital document (M) by using a plurality of partial digital signature generation parts, said distributed digital signature generation method comprising:

a partial digital signature generation step in which each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party, generates a partial digital signature by using said partial signature key for a hash value (H(M)) of an input digital document (M), and outputs said partial digital signature or a pair of said digital document and said partial digital signature;

a partial digital signature number set selecting step of assigning one of numbers from 1 to m to each of said partial digital signatures wherein m is the number of said partial digital signatures, selecting a number set I(i) including numbers ((i -1) mod m)+1,((i-1+1) mod m)+1,...,((i-1+(k-1)) mod m)+1 for each of i=1, ..., m, wherein k is a threshold necessary for generating an integrated digital signature;

an integrated digital signature generating step of combining said partial digital signatures S(i(1), M),...,S(i(k), M) to generate said integrated digital signature S(I(i), M) for each of i=1, ..., m wherein S(i, M) indicates a partial digital signature to which i is assigned and wherein elements of said number set I(i) are i(1), ..., i(k),

wherein said integrated digital signature generating step includes:

a signature verification step of performing a signature verification process for said integrated digital signature S(I(i), M) for each of i=1, ..., m to determine whether said integrated digital signature S(I(i), M) is a correct digital signature for H(M);

an incorrect partial digital signature existence determination step of determining that no incorrect partial digital signature exists in said partial digital signatures S(i, M) (i=1, ..., m) if S(I(i), M) is determined to be a correct digital signature for H(M) for every i=1, ..., m, and determining that at least an incorrect partial digital signature exists if at least one of S(I(i), M) (i=1, ..., m) is determined to be incorrect;

an incorrect partial digital signature specifying step, performed when it is determined that at least one incorrect partial digital signature exists, of determining whether a set F of i=1, ..., m agrees with a set F(j) (j is one of 1, ..., m), wherein said set F is defined to

be the set of i=1, ..., m such that S(I(i), M) is incorrect for H(M), and wherein said set F(j) is the set of i=1, ..., m by which said number set I(i) includes j, and determining that the number of said incorrect partial digital signature is only one if there is only one j by which F agrees with said set F(j), and if not, determining that the number of said incorrect partial digital signatures is equal to or greater than 2, and further, when it is determined that the number of said incorrect partial digital signature is only one, determining said only one j by which F agrees with F(j) so as to specify that said only one incorrect partial digital signature is S(j, M); and

said distributed digital signature generation method further comprising a result output step of:

when it is determined that no incorrect partial digital signature exists, outputting a determination result indicating that no incorrect partial digital signature exists and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that only one incorrect partial digital signature exists, outputting a determination result indicating that only one incorrect partial digital signature exists, identification information of said only one incorrect partial digital signature, and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that the number of said incorrect partial digital signatures is equal to or greater than 2, outputting a determination result indicating that the number of said incorrect partial digital signatures is equal to or greater than 2.

22. (New) A digitally signed digital document generation method for generating a digital document with a digital signature comprising the distributed digital signature generation method as claimed in claim 21, and further comprising the step of:

generating a digital document with digital signature which includes said digital document and said integrated digital signature.

23. (New) A distributed digital signature generation apparatus for generating a digital signature for a digital document (M) by using a plurality of partial digital signature generation parts, wherein

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party, generates

a partial digital signature by using said partial signature key for a hash value (H(M)) of an input digital document (M), and outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said distributed digital signature generation apparatus comprising:

an integrated digital signature generating part for assigning one of numbers from 1 to m to each of said partial digital signatures wherein m is the number of said partial digital signatures, selecting a number set I(i) including numbers ((i -1) mod m)+1,((i-1+1) mod m)+1,...,((i-1+(k-1)) mod m)+1 for each of i=1, ..., m, wherein k is a threshold necessary for generating an integrated digital signature; and for combining said partial digital signatures S(i(1), M),...,S(i(k), M) to generate said integrated digital signature S(I(i), M) for each of i=1, ..., m wherein S(i, M) indicates a partial digital signature to which i is assigned and wherein elements of said number set I(i) are i(1), ..., i(k),

wherein said integrated digital signature generating part includes:

a signature verification part for performing a signature verification process for said integrated digital signature S(I(i), M) for each of i=1, ..., m to determine whether said integrated digital signature S(I(i), M) is a correct digital signature for H(M);

an incorrect partial digital signature existence determination part for determining that no incorrect partial digital signature exists in said partial digital signatures S(i, M) (i=1, ..., m) if S(I(i), M) is determined to be a correct digital signature for H(M) for every i=1, ..., m, and determining that at least an incorrect partial digital signature exists if at least one of S(I(i), M) (i=1, ..., m) is determined to be incorrect;

an incorrect partial digital signature specifying part for, when it is determined that at least one incorrect partial digital signature exists, determining whether a set F of i=1, ..., m agrees with a set F(j) (j is one of 1, ..., m), wherein said set F is defined to be the set of i=1, ..., m such that S(I(i), M) is incorrect for H(M), and wherein said set F(j) is the set of i=1, ..., m by which said number set I(i) includes j, and determining that the number of said incorrect partial digital signature is only one if there is only one j by which F agrees with said set F(j), and if not, determining that the number of said incorrect partial digital signatures is equal to or greater than 2, and further when it is determined that the number of said incorrect partial digital signature is only one, determining said only one j by which F agrees with F(j) so as to specify that said only one incorrect partial digital signature is S(j, M); and

said distributed digital signature generation apparatus further comprising a result output part for:

when it is determined that no incorrect partial digital signature exists, outputting a determination result indicating that no incorrect partial digital signature exists and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that only one incorrect partial digital signature exists, outputting a determination result indicating that only one incorrect partial digital signature exists, identification information of said only one incorrect partial digital signature, and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that the number of said incorrect partial digital signatures is equal to or greater than 2, outputting a determination result indicating that the number of said incorrect partial digital signatures is equal to or greater than 2.

24. (New) A digitally signed digital document generation apparatus for generating a digital document with a digital signature comprising the distributed digital signature generation apparatus as claimed in claim 23, and further comprising:

a part for generating a digital document with digital signature which includes said digital document and said integrated digital signature.

25. (New) A program for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party, generates a partial digital signature by using said partial signature key for a hash value (H(M)) of an input digital document (M), and outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said program comprising:

integrated digital signature generating program code means for assigning one of numbers from 1 to m to each of said partial digital signatures wherein m is the number of said partial digital signatures, selecting a number set I(i) including numbers ((i -1) mod m)+1,((i-1+1) mod m)+1,...,((i-1+(k-1)) mod m)+1 for each of i=1, ..., m, wherein k is a threshold necessary for generating an integrated digital signature; and for combining said partial digital

signatures S(i(1), M),...,S(i(k), M) to generate said integrated digital signature S(I(i), M) for each of i=1, ..., m wherein S(i, M) indicates a partial digital signature to which i is assigned and wherein elements of said number set I(i) are i(1), ..., i(k),

wherein said integrated digital signature generating program code means includes:

signature verification program code means for performing a signature verification process for said integrated digital signature S(I(i), M) for each of i=1, ..., m to determine whether said integrated digital signature S(I(i), M) is a correct digital signature for H(M);

incorrect partial digital signature existence determination program code means for determining that no incorrect partial digital signature exists in said partial digital signatures S(i, M) (i=1, ..., m) if S(I(i), M) is determined to be a correct digital signature for H(M) for every i=1, ..., m, and determining that at least an incorrect partial digital signature exists if at least one of S(I(i), M) (i=1, ..., m) is determined to be incorrect;

incorrect partial digital signature specifying program code means for, when it is determined that at least one incorrect partial digital signature exists, determining whether a set F of i=1, ..., m agrees with a set F(j) (j is one of 1, ..., m), wherein said set F is defined to be the set of i=1, ..., m such that S(I(i), M) is incorrect for H(M), and wherein said set F(j) is the set of i=1, ..., m by which said number set I(i) includes j, and determining that the number of said incorrect partial digital signature is only one if there is only one j by which F agrees with said set F(j), and if not, determining that the number of said incorrect partial digital signatures is equal to or greater than 2, and further when it is determined that the number of said incorrect partial digital signature is only one, determining said only one j by which F agrees with F(j) so as to specify that said only one incorrect partial digital signature is S(j, M); and

said program further comprising result output program code means for:

when it is determined that no incorrect partial digital signature exists, outputting a determination result indicating that no incorrect partial digital signature exists and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that only one incorrect partial digital signature exists, outputting a determination result indicating that only one incorrect partial digital signature

exists, identification information of said only one incorrect partial digital signature, and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that the number of said incorrect partial digital signatures is equal to or greater than 2, outputting a determination result indicating that the number of said incorrect partial digital signatures is equal to or greater than 2.

26. (New) A computer readable medium storing a program for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party, generates a partial digital signature by using said partial signature key for a hash value (H(M)) of an input digital document (M), and outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said program comprising:

integrated digital signature generating program code means for assigning one of numbers from 1 to m to each of said partial digital signatures wherein m is the number of said partial digital signatures, selecting a number set I(i) including numbers ((i -1) mod m)+1,((i-1+1) mod m)+1,...,((i-1+(k-1)) mod m)+1 for each of i=1, ..., m, wherein k is a threshold necessary for generating an integrated digital signature; and for combining said partial digital signatures S(i(1), M),...,S(i(k), M) to generate said integrated digital signature S(I(i), M) for each of i=1, ..., m wherein S(i, M) indicates a partial digital signature to which i is assigned and wherein elements of said number set I(i) are i(1), ..., i(k),

wherein said integrated digital signature generating program code means includes:

signature verification program code means for performing a signature verification process for said integrated digital signature S(I(i), M) for each of i=1, ..., m to determine whether said integrated digital signature S(I(i), M) is a correct digital signature for H(M);

incorrect partial digital signature existence determination program code means for determining that no incorrect partial digital signature exists in said partial digital signatures S(i, M) (i=1, ..., m) if S(I(i), M) is determined to be a correct digital signature for

H(M) for every i=1, ..., m, and determining that at least an incorrect partial digital signature exists if at least one of S(I(i), M) (i=1, ..., m) is determined to be incorrect;

incorrect partial digital signature specifying program code means for, when it is determined that at least one incorrect partial digital signature exists, determining whether a set F of i=1, ..., m agrees with a set F(j) (j is one of 1, ..., m), wherein said set F is defined to be the set of i=1, ..., m such that S(I(i), M) is incorrect for H(M), and wherein said set F(j) is the set of i=1, ..., m by which said number set I(i) includes j, and determining that the number of said incorrect partial digital signature is only one if there is only one j by which F agrees with said set F(j), and if not, determining that the number of said incorrect partial digital signatures is equal to or greater than 2, and further when it is determined that the number of said incorrect partial digital signature is only one, determining said only one j by which F agrees with F(j) so as to specify that said only one incorrect partial digital signature is S(j, M); and

said program further comprising result output program code means for:

when it is determined that no incorrect partial digital signature exists, outputting a determination result indicating that no incorrect partial digital signature exists and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that only one incorrect partial digital signature exists, outputting a determination result indicating that only one incorrect partial digital signature exists, identification information of said only one incorrect partial digital signature, and said integrated digital signature determined to be correct in said signature verification step;

when it is determined that the number of said incorrect partial digital signatures is equal to or greater than 2, outputting a determination result indicating that the number of said incorrect partial digital signatures is equal to or greater than 2.